Department of Homeland Security Daily Open Source Infrastructure Report for 29 November 2006

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- KMBC−TV reports Community America Credit Union confirmed that on Friday, November 24, a hacker managed to redirect people from the company's Website to a phony site and that 180 accounts were accessed within minutes. (See item 7)
- The Associated Press reports the Modesto, California, City−County Airport was evacuated Tuesday, November 28, and flights were canceled after the city received nine bomb threats by e−mail. (See item 11)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *November 27, Daily News (TX)* — **BP to test new emergency alert system.** Testing of a new emergency alert system is scheduled at BP's Texas City refinery this week. The alert system tests at BP are slated to begin Monday, November 27, and will continue through the end of the year, company spokesperson Neil Geary said. The new system is designed to allow alerts to be heard in all parts of the 1,200−acre facility. It is also likely people within 2,000 feet of the refinery will hear the siren system, Geary said. The new alert system, which is a combination of sirens, pager alerts, and internal video communication, comes in response to the March 23, 2005 explosions in which 15 people were killed and more than 170 injured. Federal

investigations and BP’s internal assessment found an inadequate emergency alert system existed in the refinery prior to the fatal blasts.
Source: http://news.galvestondailynews.com/story.lasso?ewcd=a0ea27ce 4245dca4

2. *November 27, Houston Chronicle* — **Big expansion points to role of Gulf refining.** A year ago at this time, Motiva's sprawling refinery in Port Arthur, TX, was still cleaning up an epic mess left by Hurricane Rita. Today, this facility is girding for an expansion that will double its capacity to 600,000 barrels per day and could make it the largest refinery in the nation by 2010. The project shows that when decisions are made about refinery expansions, the industry's long history and its vast infrastructure along the Gulf Coast continue to outweigh most other concerns, including hurricanes. This $3.5 billion project also shows why refiners are choosing to expand existing facilities rather than start from scratch. As huge and complicated as the project is, it will still be less expensive than building a new facility at a new site. Refiners have announced plans to boost capacity by almost two million barrels by 2010, or about 11 percent above the current rate. The flurry of activity has been fueled by high crude prices, rising energy demands and strong refining profit margins, leading one Wall Street analyst to dub the 2004−to−2006 period the "Golden Age of Refining."
Source: http://www.chron.com/disp/story.mpl/business/energy/4363797. html

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *November 28, Aviation Now* — **Different communication networks for Raptor eyed by Air Force.** The U.S. Air Force is scrutinizing different communication networks to help make the F−22 Raptor a better aircraft for intelligence, surveillance and reconnaissance, as well as command and control. While service leaders have been touting the Raptor's ability to shine in these types of missions, F−22 pilots acknowledge the aircraft has shortcoming in those roles. In a recent interview at Tyndall Air Force Base, FL, Maj. Shawn "Rage" Anger, an F−22 instructor with the 43rd Fighter Squadron, said the Raptor still can't share some of the most detailed information through its communication links. Pilots can't offload the symbology and other screen information that gives the complete battlespace picture. One future possibility, he acknowledged, would be to use the radar as a high−bandwidth communications link to transmit more data. Gen. Ronald Keys, commander of Air Combat Command at Langley Air Force Base, VA, acknowledged the shortcoming and said the Air Force is considering other waveforms and networks to help the Raptor share that kind of information.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily _story.jsp?id=news/RAPT11286.xml

[Return to top]

Banking and Finance Sector

4. *November 28, CNET News* — **Google search apps packing 'phishing flaw'.** A security flaw in Google's search appliances could expose Websites that use the products to info−stealing phishing attacks, experts have warned. The Google Search Appliance and Google Mini are used by organizations including banks and universities to add search features to Websites. A flaw in the way the systems handle certain characters makes it possible to craft a Web link that looks as if it points to a trusted site but when clicked serves up content from a third, potentially malicious site. John Herron, a security expert who maintains the NIST.org site, said: "This vulnerability affects a lot of very large Websites. It basically allows a virtual defacement of a Website when following a malicious link." Google notified all customers on November 22 with clear instructions on how to protect their appliances. The vulnerability will also be addressed in the next release of the products. No Google Search Appliance or Google Mini users have reported any exploits of the flaw. The cross−site scripting problem involves 7−bit Unicode Transformation Format (UTF) character encoding. The rigged links will be very long, according to security experts. Users who have not heard from Google should contact the company for a fix.
   Source: http://software.silicon.com/security/0,39024888,39164382,00. htm

5. *November 27, Business Journal of the Greater Triad Area (NC)* — **State bankers prepare for bird flu.** The North Carolina Bankers Association is planning a seminar designed to help financial institutions prepare for a possible pandemic, including a possible outbreak of avian influenza in humans. According to the association, a pandemic could have disastrous economic consequences for which bankers need to prepare. "Despite advances in medical technology and therapies, the Congressional Budget Office warns that a severe pandemic could cause two million American deaths and up to five percent drop in the gross domestic product," the announcement said. The seminar, which will take place December 5 in Durham, NC, will feature discussion of both the science behind how the bird flu could transfer to humans and how the banking industry should react to the public health threat. N.C. Banking Commissioner Joe Smith said, "Bankers and their regulators have an obligation to prepare for this threat and have plans ready to deal with it effectively."
   Source: http://triad.bizjournals.com/triad/stories/2006/11/27/daily1 .html

6. *November 27, Finextra (UK)* — **Security fears scare off U.S. customers from online banking, shopping.** Nearly $2 billion in U.S. e−commerce sales will be lost in 2006 due to consumer concerns over the security of the Internet, according to a survey by Gartner, which also found that fear of fraud and identity theft have prevented around 33 million U.S. adults from banking online. The survey of 5,000 online US adults in August 2006 found that recent security breaches −− both online and offline −− are having a significant impact on buying patterns and use of Web banking facilities. Nearly half of those surveyed (46 percent) said concerns about theft of information, data breaches or Internet−based attacks have affected their purchasing payment, online transaction or e−mail behavior. Of all the behaviors affected, online commerce −− which includes Internet banking, online payments and Web shopping −− is suffering the most. Almost nine million U.S. adults have stopped using online banking, while another estimated 23.7 million won't even start because of fears over security.
   Source: http://finextra.com/fullstory.asp?id=16204

7. *November 27, KMBC−TV 9 (KS)* — **Hacker redirects bank customers to phony site; 180 accounts accessed within minutes.** Community America Credit Union confirmed that on Friday, November 24, a hacker managed to redirect people from the company's Website to a phony site. Community America said it caught the intrusion within a few minutes, but that was enough for the hacker to get information to access 180 accounts.
Source: http://www.thekansascitychannel.com/money/10408223/detail.ht ml

[Return to top]

Transportation and Border Security Sector

8. *November 28, Today's Trucking (Canada)* — **Three Lower Mainland ports agree to merge.** The Lower Mainland's three gateway port authorities have ratified a report recommending each port facility merge into a single Canada Port Authority. The boards of the Vancouver, North Fraser, and Fraser River port authorities commissioned the report by InterVISTAS Consulting Ltd. The group was tasked with finding ways for the Lower Mainland ports to explore opportunities that will allow them to become even more globally competitive and capture a larger share of growing Pacific trade volumes. "The report confirms that integration of port activities in the Lower Mainland can enhance Canada's competitiveness in the global trade environment, and is the most effective means of optimizing port planning, development and marketing," said Vancouver Port Authority Chair George Adams.
Source: http://www.todaystrucking.com/news.cfm?intDocID=17056

9. *November 28, Tucson Citizen (AZ)* — **Tucson Airport Authority approves $35M in bonds.** The Tucson Airport Authority (TAA) approved the sale of $35 million in bonds on Tuesday, November 28, to finance the concourse renovations in the coming year at Tucson International Airport (TIA). The $4.50 passenger facility charge that each passenger flying out of TIA pays should pay off about 79 percent of the bonds with airport revenues covering the balance, said Dick Gruentzel, TAA's vice president of finance and administration. The $31 million renovation will reconfigure the security checkpoint areas as well as replace all the seating and carpet in both concourses and creating a new lounge area for people waiting for customers. Work is expected to start in December at the security checkpoints and move into the west concourse in about March and into the east concourse in summer.
Source: http://www.tucsoncitizen.com/daily/local/34046.php

10. *November 28, Seattle Post−Intelligencer* — **Slow commute leads to airport backups.** A crush of passengers and bad commuting conditions resulted in long security lines Tuesday morning, November 28, at Seattle−Tacoma Airport (Sea−Tac). A number of Transportation Security Administration (TSA) staffers, who check baggage and passengers before they board planes, were late to work because of cold weather and icy roads, said TSA spokesperson Jennifer Peppin. As a result, there was just one checkpoint operating at 5 a.m. PST; normally there are at least two and sometimes more. In addition, she said, there were between 5,000 and 10,000 travelers stranded at the airport overnight, unable to leave. The stranded people −− plus the 40,000 travelers expected to use the airport during the day −− "adds a huge crush first thing in the morning," Peppin said. Peppin advised travelers to call before coming to the airport to make sure flights were on time.
Source: http://seattlepi.nwsource.com/local/293914_commute28ww.html

11. *November 28, Associated Press* — **California airport evacuated, flights canceled after bomb threats.** The Modesto City−County Airport was evacuated Tuesday, November 28, and flights were canceled after the city received nine bomb threats by e−mail, police said. About 50 passengers and employees were evacuated, and at least one morning commuter flight was affected, Modesto police Sgt. Craig Gundlach said. Police and federal officials used bomb−sniffing dogs midday to sweep the terminal and airport. The city's Web master received the threatening e−mails early in the morning but authorities did not immediately release information about who sent the threats or possible motives. The FBI, Transportation Security Administration, and the Bureau of Alcohol, Tobacco, Firearms and Explosives were investigating.
Source: http://www.montereyherald.com/mld/montereyherald/news/161161 33.htm

12. *November 27, Department of Transportation* — **DOT provides emergency funding to Washington State.** Accompanied by Senator Patty Murray and Washington Governor Christine Gregoire, Transportation Secretary Mary E. Peters announced on Monday, November 27, that the state of Washington will immediately receive $1 million in emergency relief funding to help repair roads, bridges and tunnels across the state. This “quick−release” funding is intended as a first installment in reimbursing the state for costs associated with damage caused by recent heavy rainfall and flooding in the Pacific Northwest, the Secretary said. Total cost estimates are still underway, and the state remains eligible for additional federal funding should damages exceed this first disbursement. Once these estimates are completed, the Department will work with the state to provide all eligible additional funding. The Federal Highway Administration’s (FHWA) Emergency Relief program is designed to reimburse states for certain costs −− up to $100 million per state per disaster −− resulting from natural disasters or other emergencies. The funds can be used for reconstructing or replacing damaged highways and bridges, removing debris, creating detours and fixing or replacing signs, lighting and guardrails.
Details about the FHWA’s Emergency Relief program:
http://www.fhwa.dot.gov/programadmin/erelief.html
Source: http://www.dot.gov/affairs/dot10806.htm

13. *November 27, Associated Press* — **Mesaba unions approve new contracts.** Unions at Mesaba Aviation Inc. said Monday, November 27, they have approved new concessionary contracts with the bankrupt airline, a Northwest Airlines feeder. About 1,100 pilots, flight attendants and mechanics are covered by the contracts, which took nearly a year to reach and brought the unions to the brink of a strike. Mesaba said it needed the labor deals to continue handling regional flying for Northwest Airlines Corp., which also is operating in bankruptcy. Mesaba earlier got permission from a bankruptcy judge to impose cuts amounting to 17.5 percent of pay and benefits on the union, but held off as the two sides continued bargaining. Union leaders said they weren't happy with the deal, but that it was necessary to keep Mesaba flying and preserve jobs for their members. Mesaba's management issued a statement saying the agreements were necessary to emerge from bankruptcy. Mesaba flies to 88 cities, funneling passengers into Northwest hubs in Detroit, Minneapolis, and Memphis. Its fleet once numbered about 100 planes, including regional jets, but Northwest has reduced that to 49 prop−driven Saab aircraft.
Source: http://biz.yahoo.com/ap/061127/mesaba_labor.html?.v=18

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

14. *November 27, Dow Jones* — **Plan to lift older Canada cattle ban resubmitted to OMB.** The White House Office of Management and Budget (OMB) has once again been tasked with reviewing the U.S. Department of Agriculture's (USDA) plan to lift its ban on older Canadian cattle, deemed riskier for mad−cow disease infection than younger animals. The U.S. now only allows for the importation of cattle −− and beef derived from them −− that are under 30 months old. The U.S. banned all Canadian beef and cattle in May 2003 after Canada's first domestic case of bovine spongiform encephalopathy (BSE) was found. The USDA eased that ban a few months later on some beef and, in July 2005, began allowing in younger cattle that represent most imports. The USDA proposal to allow in older cattle has taken longer because older cattle are believed to be at higher risk for BSE.
Source: http://www.agriculture.com/ag/futuresource/FutureSourceStoryIndex.jhtml?storyId=74100486

15. *November 27, Horse* — **Wisconsin offering voluntary animal ID cost sharing program.** The state of Wisconsin is inviting livestock producers to participate in a voluntary animal identification program. With a premises registration system in place, the state wishes to support those producers who are ready to begin recording individual animal ID and animal movement information as the next steps of the National Animal Identification System. The Wisconsin Department of Agriculture is offering a Voluntary Animal ID Cost Sharing Program on a first come, first serve basis to producers interested in doing their part in managing a potential animal disease outbreak in Wisconsin. The program consists of sign−up, approval, and confirmation of participation followed by tag purchase and application. Reimbursement is made once these steps have been completed. A producer must have a premises registration number to qualify for the program.
Source: http://www.thehorse.com/viewarticle.aspx?ID=8250

16. *November 21, Southeast Farm Press* — **New weed pest threatens Carolina field crops.** Commelina benghalensis, commoly called Benghal dayflower, or spiderwort, has been found in several southern states and may become a threat to South Carolina growers in 2007 and possibly North Carolina growers in subsequent years. Benghal dayflower is a double threat in that it can produce seeds from both above and below ground sites. It is tolerant of glyphosate and many other commonly used herbicides. Once it gets a start from ditches or irrigation banks, it can rapidly spread through cultivated fields causing severe yield losses in field crops.
Source: http://southeastfarmpress.com/news/112206−dayflower−threat/

[Return to top]

Food Sector

17. *November 28, Express−News (TX)* — **CDC issues alert on queso fresco.** They are staples of traditional Hispanic cuisine −− fresh cheeses with names like queso blanco, panela and queso fresco. The soft, creamy concoctions have devoted followings on both sides of the border, but health officials are renewing warnings that the popular versions made from raw milk can seriously sicken people and even cause death. A new scientific report by the Centers for Disease Control and Prevention (CDC) warns that imports of unpasteurized cheeses from Mexico continue despite frequent health warnings about consuming the products. Mexican and U.S. health and agriculture officials have been working recently on improving communication to better control outbreaks along the border, said Dr. Stephen Waterman, a CDC medical epidemiologist based in California. Problems arise when people either smuggle in or are allowed to bring large amounts of unpasteurized cheeses into the country from Mexico that they then resell, he said.
Source: http://www.mysanantonio.com/news/metro/stories/MYSA112806.01A.NZ.Metro.whitecheese.3590646.html

18. *November 27, Baltimore Sun* — **Parasite puts Asian oysters at risk.** Researchers have concluded that Asian oysters are susceptible to a parasite that could wipe them out if they were ever planted in the Chesapeake Bay, raising new concerns about a proposal to use the foreign species to revive the region's struggling seafood industry. The research found that Asian oysters experienced "almost total mortality" when exposed to the parasite Bonamia from the earliest stages of life, said Ryan Carnegie, a scientist at the Virginia Institute of Marine Science, where the study is being done. A plan was proposed by Maryland Governor Robert Ehrlich Jr. to introduce Asian oysters into the bay to help filter the increasingly polluted water and to give struggling watermen a crop to harvest. Diseases and over−harvesting have all but destroyed the native oyster populations in the bay. Scientists are concerned that the parasite would make introduction of Asian oysters a poor investment. "If, in five years, we had a very active aquaculture industry, then you could have enough hosts for the disease to take hold," said Roger Newell, an oyster biologist and the University of Maryland's Center for Environmental Science. "You could all get geared up for this wonderful, oyster−industry−saving species, and then it nails you."
Source: http://www.baltimoresun.com/news/local/bal−md.asianoysters27nov27,0,7854280.story?coll=bal−local−headlines

19. *November 24, Scripps Howard News Service* — **Study: U.S. vulnerable to food−borne illnesses.** More than 50,000 people got sick or died from something they ate in a hidden epidemic that went undiagnosed by the nation's public health departments over a five−year period. Americans play a sort of food−poisoning Russian roulette depending on where they live, an investigation by Scripps Howard News Service found. Slovenly restaurants, disease−infested food−processing plants, and other sources of infectious illness go undetected all over the country, but much more frequently in some states than others. Scripps studied 6,374 food−related disease outbreaks reported by every state to the federal Centers for Disease Control and Prevention from January 1, 2000, through December 31, 2004. The causes of nearly two−thirds of the outbreaks in that period were officially listed as "unknown." If health officials are unable to connect illness to food, victims who might eat from the same poisoned

source cannot be warned. If food is known as the culprit, but the specific disease lurking within is not diagnosed, the victims may get even sicker or die without proper treatment. The poor track record of so many state labs also raises chilling questions about their ability to spot or deal with a food−borne terrorist attack.
Source: http://www.detnews.com/apps/pbcs.dll/article?AID=/20061124/LIFESTYLE03/611240346/1040&template=printart

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

20. *November 28, News−Medical (Australia)* — **New bird flu drug will provide new line of defense.** Flu experts say a new flu drug with the ability to kill deadly strains of bird flu promises to provide a much needed third option should a pandemic occur. The anti−viral agent Peramivir may well offer a vital new line of defense against the deadly the H5N1 avian strain. Peramivir could totally transform global preparations for an influenza pandemic as it has been seen in studies to be more powerful and easier to deliver than either Tamiflu or Relenza, the two existing drugs for H5N1 flu. Apparently where Peramivir has the advantage over the other therapies is that it is delivered as an injection while Tamiflu must be taken orally, and Relenza must be inhaled; both therapies are difficult when patients are unconscious. Also, because Peramivir is injected it enters the bloodstream in higher concentrations and remains active for longer.
Source: http://www.news−medical.net/?id=21117

21. *November 28, Reuters* — **South Korea confirms second H5N1 bird flu case.** South Korea on Tuesday, November 28, confirmed a second outbreak of the H5N1 strain of bird flu at a poultry farm, after confirming over the weekend it had its first outbreak in three years of the strain that can kill people. The agriculture ministry said about 600 chickens died in the latest outbreak at a farm two miles from where the first case had been confirmed in poultry in North Cholla province in the country's southwest. Quarantine authorities will cull all poultry within a 1,640 feet radius of the latest infected farm.
Source: http://www.alertnet.org/thenews/newsdesk/SEO155054.htm

22. *November 28, Associated Press* — **Indonesian woman dies of bird flu, raising country's death toll to 57.** An Indonesian woman died of bird flu Tuesday, November 28, raising the country's death toll to 57. The 35−year−old woman had been treated for almost three weeks before dying in a hospital in the capital, Jakarta, said hospital spokesperson Sardikin Giriputro. Health officials were still investigating the source of infection. Indonesian Health Ministry tests earlier this month confirmed that the woman from the city of Tangerang, on the western outskirts of Jakarta, was H5N1 positive.
Source: http://www.usatoday.com/news/health/2006−11−28−indonesia−bir d−flu_x.htm

23. *November 27, Reuters* — **Japanese scientists claim to have identified anti−TB compound.** Scientists in Japan say they have identified a compound that appears to stop the tuberculosis (TB) bacteria from multiplying, offering new hope in the fight against the increasingly drug−resistant disease. At least a third of the world's population is estimated to be infected with the TB bacteria, which are protected by a thick waxy coat and can lie dormant for years. People who are infected normally only get sick when their immune systems are weak. In an article published in the open access journal, PLoS Medicine, the researchers tested the compound, OPC−67683, on infected mice. It attacked the walls of the bacteria and "stopped it from dividing further," said Makoto Matsumoto of Otsuka Pharmaceutical Co. Ltd.'s Microbiological Research Institute. The compound was also effective in fighting multi−drug resistant strains of TB, he said.
Study: http://medicine.plosjournals.org/perlserv/?request=get−document&doi=10.1371/journal.pmed.0030466
Source: http://health.yahoo.com/news/169278;_ylt=ApLvFjiDTNZlV_xpe_h.lPCmxbAB

24. *November 25, Reuters* — **Sri Lanka confirms Chikungunya viral fever epidemic.** Sri Lanka has confirmed an epidemic of the mosquito−borne Chikungunya viral fever, a top health official said on Saturday, November 25. Doctors suspect it has infected 5,000 people in the island's far north. Dr. Nihal Abeysinghe, director of the state Epidemiology Department, said pockets of the fever had been detected in Sri Lanka's northwest, south and east, but could not say how many cases had been reported. The outbreak comes as Sri Lanka also grapples with a sharp increase in dengue fever cases as monsoon rains create breeding conditions for mosquitoes which carry the diseases.
Source: http://today.reuters.com/news/articlenews.aspx?type=healthNews&storyID=2006−11−25T083544Z_01_COL171374_RTRUKOC_0_US−SRILANKA−EPIDEMIC.xml&WTmodLoc=NewsArt−C2−NextArticle−1

[Return to top]

Government Sector

25. *November 28, Herald News (MA)* — **Bomb squad called to Fall River, Massachusetts, Government Center.** Hundreds of federal, state, and city workers were evacuated from their buildings early Monday afternoon, November 27, after a suspicious package was found on the steps of the Fall River Government Center. Fall River Police Lt. Gene Rodrigues said police were called to the scene at about 12:30 p.m. EST with reports of the suspicious package. Witnesses at the scene reported that at least two Government Center workers saw a man making numerous threats in the building earlier in the day, but the specific threats were not reported by police. An hour after the threats were made, police said the package appeared on the steps. "We have to evacuate everyone within the 500−foot perimeter," said Rodrigues, which included Government Center, the post office, and the Citizens−Union Bank. The X−rays showed nothing out of the ordinary inside the case. Rodrigues said a similar event occurred two weeks ago when a package was left in front of the post office steps. Bomb technician trooper Scott Fahey said his Massachusetts squad goes on approximately 500 bomb−related calls each year.
Source: http://www.heraldnews.com/site/news.cfm?newsid=17519361&BRD=1710&PAG=461&dept_id=99784&rfi=6

[Return to top]

Emergency Services Sector

26. *November 27, Associated Press* — **First responders learning Spanish.** Everyday, emergency responders and law enforcement officers nationwide help non−English−speaking people whose lives might be in immediate danger. The job is particularly challenging for small agencies in the South, which has seen a recent influx of Hispanic residents. Many dispatchers and officers are going out of their way to learn Spanish and departments are recruiting bilingual employees and buying translating technology as they adapt to changing demographics. With increasing pressure on police to help enforce immigration laws, tensions between immigrants and officers run high and the language barrier hurts both. In border states like Arizona, long accustomed to a strong Hispanic presence, some agencies resent the added pressure of learning a new language, but most officers are trying to understand and make themselves understood.
Source: http://www.chron.com/disp/story.mpl/ap/nation/4361878.html

27. *November 27, Washington Technology* — **HHS working on emergency−responder health IT use.** Details of an emergency−responder electronic health record as another early use for health IT are being developed by the Health and Human Services Department (HHS). The need arose out of lessons learned from Hurricane Katrina, during which emergency providers had to assemble patient histories and medications with little information because flood waters had destroyed medical records. Following the disaster, a federal study recommended use of interoperable electronic health records systems for use by emergency responders. Development of an emergency−responder electronic health record system would focus on the critical health information related to assessing, stabilizing and treating victims of emergencies, such as accidents and large group casualties. It would include minimum demographic, medication, allergy and problem list information.
Source: http://www.washingtontechnology.com/news/1_1/daily_news/29763−1.html?topic=homeland

28. *November 26, Reuters* — **World neglects tsunami risk lessons: Red Cross.** The world could see a replay of the massive death and destruction caused by the December 2004 Indian Ocean tsunami if it fails to spend more on disaster risk reduction, the Red Cross/Red Crescent said on Monday, November 27. The tsunami that left more than 200,000 people dead or missing around the Indian Ocean should have taught the value of preparedness, but "risk reduction has remained low on the international agenda," the International Federation of Red Cross and Red Crescent Societies said in a statement. It called for a rise in annual disaster preparedness global spending to $1 billion, 10 percent of the amount spent on humanitarian aid. The figure is now around four percent. Too often "when the first assessment of damage is done and the costing of reconstruction after an earthquake or some other disaster is done, risk reduction is not immediately factored in," Johan Schaar, federation special representative for the tsunami, told Reuters. Aside from the potential lives to be saved, the federation estimates a dollar spent on prevention can save as much as $10 in reconstruction and rebuilding costs.
Source: http://www.alertnet.org/thenews/newsdesk/SP290805.htm

[Return to top]

Information Technology and Telecommunications Sector

29. *November 27, Reuters* — **E−mail gangs bombard Britain with spam.** Criminal gangs using hijacked computers are behind a surge in unwanted e−mails peddling sex, drugs and stock tips in Britain. The number of "spam" messages has tripled since June and now accounts for as many as nine out of 10 e−mails sent worldwide, according to U.S. e−mail security company Postini. Postini has detected 7 billion spam e−mails worldwide in November compared to 2.5 billion in June. Spam in Britain has risen by 50 percent in the last two months alone, according to Internet security company SurfControl. The United States, China and Poland are the top sources of spam, data from security firm Marshal suggests. About 200 illegal gangs are behind 80 percent of unwanted e−mails, according to Spamhaus, a body that tracks the problem. Experts blame the rise in spam on computer programs that hijack millions of home computers to send e−mails.
Source: http://www.eweek.com/article2/0,1895,2064450,00.asp

30. *November 27, Associated Press* — **EU says more than half e−mails are spam.** Unsolicited e−mails continue to plague Europeans and account for between 50 and 80 percent of all messages sent to mail inboxes, the European Commission said Monday, November 27. A European Union (EU) report found that only two EU nations −− the Netherlands and Finland −− were making inroads in enforcing the 2002 law to crack down on spam. Dutch authorities were able to reduce spam by 85 percent by using fines to get businesses to fall in line with the EU rule. EU officials have said they will put forward new legislation next year to make it easier to prosecute spammers.
Source: http://news.yahoo.com/s/ap/20061128/ap_on_hi_te/eu_spam

31. *November 27, ZDNet Asia* — **Hackers ride on Web application vulnerabilities.** According to Watchfire, the most vulnerable area in the enterprise information ecosystem is Web applications. The company specializes in software and services to audit the security and regulatory compliance of Websites. Danny Allan, Watchfire's director of strategic research, noted that network perimeters bore the brunt of attacks in the past. Given that networks today are adequately protected by a range of security tools, Web applications are now not only easier to target, they are also linked to backend servers and databases containing a wealth of information. However, businesses are currently not spending enough to protect their Web applications, said Allan. Citing research by Gartner, he pointed out that 90 percent of IT security spending is on network protection and only 10 percent is spent on Web applications.
Source: http://www.zdnetasia.com/news/security/0,39044215,61969925,0 0.htm

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	4662 (eDonkey2000), 1026 (win−rpc), 6881 (bittorrent), 4672 (eMule), 1027 (icq), 1028 (−−−), 25 (smtp), 50001 (−−−), 32796 (−−−), 113 (auth) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer